UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/741,103 | 12/21/2000 | W. David Shambroom | 96-3-512CON1CIP1 | 6686 |

26615 7590 07/27/2005

HARRITY & SNYDER, LLP
11240 WAPLES MILL ROAD
SUITE 300
FAIRFAX, VA 22030

| EXAMINER | |
|---|---|
| BAUM, RONALD | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

DATE MAILED: 07/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. 09/741,103 | Applicant(s) SHAMBROOM, W. DAVID | |
|---|---|---|---|
| | Examiner Ronald Baum | Art Unit 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *05 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is in reply to applicant's correspondence of 05 April 2005.

2. Claims 1-37 are pending for examination.

3. Claims 1-37 remain rejected.

### *Specification*

The disclosure is objected to because of the following informalities: the specification on page 1, line 5 is missing the status change of application 09/309,695 to issued patent 6,198,824.

Appropriate correction is required.

### *Double Patenting*

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-37 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-13 of U.S. Patent No. 6,198,824 B1. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-37 of the instant application are envisioned by copending patent claims 1-13 in that claims 1-13 of the patent contains all the limitations of claims 1-37 of the instant application. Claims 1-37 of the instant application therefore are not patently distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting.

Claims 1-37 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-27 of U.S. Patent No. 5,923,756. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-37 of the instant application are envisioned by copending patent claims 1-27 in that claims 1-27 of the patent contains all the limitations of claims 1-37 of the instant application. Claims 1-37 of the instant application therefore are not patently distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for

patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-37 remain rejected under 35 U.S.C. 102(e) as being anticipated by Wu et al, U.S. Patent 5,774,551.

5. As per claim 1; "A method for providing secure communication of commands from a client to a plurality of hosts via a network server [figure 1,3-5 and accompanying descriptions], comprising:

utilizing

authentication information and

credentials cache information within the network server

to facilitate the secure communications,

wherein

the authentication information is erased and

the credentials cache information is destroyed after the utilizing [col. 1,lines14-col. 3,line 17, col. 4,lines 3-24, col. 5,lines 7-col. 6,line 12, table 1 and associated description, col. 11,lines 56-col. 12,line 20, col. 15,lines 25-col. 21,line 29, whereas the use of the client , server, hosts system where the authentication service destroys the users credentials and authentication tokens, and, the said users credentials and authentication tokens are removed from the storage facility, clearly encompasses the claims limitations "... utilizing authentication ... credentials cache ... server ... the authentication ... erased ... credentials ... destroyed after the utilizing", as broadly interpreted by the examiner.];

receiving at least one command from the client [col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, (i.e., the FTP, TELNET request/response inclusive of the authentication sequence)];

initiating one or more remote execution processes for

processing the at least one command [col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication processing at the various remote host computers (i.e., database, applications servers) clearly constitutes a remote execution process];

transmitting the at least one command to

one or more of the hosts via

the one or more remote execution processes [col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication processing at the various remote host computers (i.e., database, applications servers) clearly constitutes a remote execution process];

obtaining, from the one or more remote execution processes,

data associated with the one or more hosts executing the at least one command [col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication process will clearly produce a result that is sent back through the communications path];

formatting the data [col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication process will clearly produce a result that is sent

back through the communications path in some specified and pre-designated or standard format]; and

sending the formatted data to

the client [col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication process will clearly produce a result that is sent back through the communications path in some specified and pre-designated or standard format].";

Further, as per claim 13; this claim is the system claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

Further, as per claim 14; this claim is the software computer-readable medium claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

Further, as per claim 26; this claim is the server part of the system claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

6. Claim 2 ***additionally recites*** the limitation that; "The method of claim 1, further comprising:

determining a maximum number of remote execution processes that may run simultaneously.".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the central server system clearly determines "who" it's communicating with (i.e., the number of such

network nodes) so that the server knows what to control (i.e., "who" is authenticated), and therefore sent commands associated with the access to resources, etc.);

Further, as per claim 15; this claim is the software computer-readable medium claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection;

Further, as per claim 27; this claim is the server part of the system claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection.

7. Claim 3 ***additionally recites*** the limitation that; "The method of claim 2, wherein the initiating includes:

creating no more than the maximum number of remote execution processes to process the at least one command. ".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the central server system clearly determines "who" it's communicating with (i.e., the number of such network nodes) so that the server knows what to control (i.e., "who" is authenticated), and therefore sent commands associated with the access to resources, etc.), and clearly, as for the case for TELNET, is a specific (i.e., a maximum number) of open TELNET communications channels.);

Further, as per claim 16; this claim is the software computer-readable medium claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection;

Further, as per claim 28; this claim is the server part of the system claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection.

8. Claim 4 ***additionally recites*** the limitation that; "The method of claim 1, further comprising:

determining whether any of the one or more remote execution processes is running.".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication process will clearly produce a result that is sent back through the communications path, and further, the central server system clearly determines "who" it's communicating with (i.e., the number of such network nodes) so that the server knows what to control (i.e., "who" is authenticated), and therefore sent commands associated with the access to resources, etc.);

Further, as per claim 17; this claim is the software computer-readable medium claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection;

Further, as per claim 29; this claim is the server part of the system claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection.

9. Claim 5 ***additionally recites*** the limitation that; "The method of claim 4, wherein the obtaining data includes:

waiting for one of the one or more remote execution processes to exit, and

storing data from the one remote execution process.".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication process will clearly produce a result that is sent back through the communications

path, and further, the remote servers inherently will store data associated with the state(s) of any ongoing processing (i.e., building a formatted message (results of authentication) prior to communicating such information back through the communications path.);

Further, as per claim 18; this claim is the software computer-readable medium claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection;

Further, as per claim 30; this claim is the server part of the system claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection.

10. Claim 6 ***additionally recites*** the limitation that; "The method of claim 1, wherein the formatting includes:

grouping data from each of the one or more remote execution processes, and

serializing the data.".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication process will clearly produce a result that is sent back through the communications path in some specified and pre-designated or standard format. Further, since the network communications (i.e., remote servers/computer nodes to central (multiple logon) server to client server/computer node) is via secure transport layer protocol (ISO TCP/IP), the format of the data returning is inherently serial as to the packet to packet transfer following the authentication for each network node involved in the secure communications setup (i.e., authentication of passwords, etc.).);

Further, as per claim 19; this claim is the software computer-readable medium claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection;

Further, as per claim 31; this claim is the server part of the system claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection.

11. Claim 7 ***additionally recites*** the limitation that; "The method of claim 1, further comprising:

determining that another remote execution process needs to be initiated; and

initiating the other remote execution process.".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication processing at the various remote host computers (i.e., database, applications servers) clearly constitutes a remote execution process initiated. The system is clearly configured on a demand basis such that a second, and further subsequent, command would require further authentication, and therefore additional remote execution process initiations.);

Further, as per claim 20; this claim is the software computer-readable medium claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection;

Further, as per claim 32; this claim is the server part of the system claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection.

12. Claim 8 ***additionally recites*** the limitation that; "The method of claim 1, wherein the initiating includes:

creating a list of the one or more remote execution processes that have been initiated.". The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication process will clearly produce a result that is sent back through the communications path, and further, the remote servers inherently will store data associated with the state(s) of any ongoing processing (i.e., building a formatted message (results of authentication) prior to communicating such information back through the communications path. It is inherent that the data structures of computers processing multiple instances (i.e., the state of remote execution processes) would be organized in a "list" structure, either in memory, or stored in mass storage (i.e., hard drive or equivalent mass storage media).);

Further, as per claim 21; this claim is the software computer-readable medium claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection;

Further, as per claim 33; this claim is the server part of the system claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection.

13. Claim 9 ***additionally recites*** the limitation that; "The method of claim 8, further comprising:

setting a time of an alarm event; and

obtaining a status of the one or more remote execution processes on the list when the alarm event occurs.".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the

authentication processing at the various remote host computers (i.e., database, applications servers) clearly constitutes a remote execution process, and further, the use of "... Each account service 111 includes methods that set and get account validation attributes, including authentication token *aging* information, such as when the authentication token *expires*, ... number of valid days, and the like; access hours restrictions for the user's account; account expiration date; and account service restrictions, such as what directories, file, resource, or services the user is authorized to access. ..." utilizes expiration as an alarm condition, typically as a result of connection/acknowledgement setup.);

Further, as per claim 22; this claim is the software computer-readable medium claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection;

Further, as per claim 34; this claim is the server part of the system claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection.

14. Claim 10 ***additionally recites*** the limitation that; "The method of claim 9, wherein the obtaining a status includes:

determining whether the next remote execution process has been running for a first amount of time, and

terminating the next remote execution process when the next remote execution process has been running for at least the first amount of time.".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication processing at the various remote host computers (i.e., database, applications

servers) clearly constitutes a remote execution process, and further, the use of "... Each account service 111 includes methods that set and get account validation attributes, including authentication token *aging* information, such as when the authentication token *expires*, ... number of valid days, and the like; access hours restrictions for the user's account; account expiration date; and account service restrictions, such as what directories, file, resource, or services the user is authorized to access. ..." utilizes expiration as an alarm condition, typically as a result of connection/acknowledgement setup. The examiner broadly interprets the "determining whether the next remote execution process has been running for a first amount of time, and terminating the next remote execution process when the next remote execution process has been running for at least the first amount of time" as the re-attempting of the authentication process, such that the scenario is effectively a serial authentication process with a alarm condition result reporting aspect.);

Further, as per claim 23; this claim is the software computer-readable medium claim for the method claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection;

Further, as per claim 35; this claim is the server part of the system claim for the method claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection.

15. Claim 11 ***additionally recites*** the limitation that; "The method of claim 10, wherein the obtaining a status further includes:

determining whether the next remote execution process has been running for a second amount of time, the second amount of time being less than the first amount of time, and

setting a next alarm event when the next remote execution process has been running the second amount of time.".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication processing at the various remote host computers (i.e., database, applications servers) clearly constitutes a remote execution process, and further, the use of "... Each account service 111 includes methods that set and get account validation attributes, including authentication token *aging* information, such as when the authentication token *expires*, ... number of valid days, and the like; access hours restrictions for the user's account; account expiration date; and account service restrictions, such as what directories, file, resource, or services the user is authorized to access. ..." utilizes expiration as an alarm condition, typically as a result of connection/acknowledgement setup. The examiner broadly interprets the "determining whether the next remote execution process has been running for a first amount of time, and terminating the next remote execution process when the next remote execution process has been running for at least the first amount of time" as the re-attempting of the authentication process, such that the scenario is effectively a serial authentication process with a alarm condition result reporting aspect.). Further, the examiner broadly interprets the "...setting a next alarm event when the next remote execution process has been running the second amount of time..." to be the sequentially occurring event where a second serial authentication process with a alarm condition result reporting aspect error occurs.);

Further, as per claim 24; this claim is the software computer-readable medium claim for the method claim 11 above, and is rejected for the same reasons provided for the claim 11 rejection;

Further, as per claim 36; this claim is the server part of the system claim for the method claim 11 above, and is rejected for the same reasons provided for the claim 11 rejection.

16. Claim 12 ***additionally recites*** the limitation that; "The method of claim 11, wherein the obtaining data includes:

storing data from the next remote execution process when the next remote execution process has been running less than the first amount of time but at least the second amount of time.".

The teachings of Wu et al suggest such limitations (figure 1,3-5 and accompanying descriptions, col. 3,line 19-55, col. 4,lines 62-col. 8,line 44, col. 17,lines 1-col. 19,line 56, whereas the authentication processing at the various remote host computers (i.e., database, applications servers) clearly constitutes a remote execution process, and further, the use of "... Each account service 111 includes methods that set and get account validation attributes, including authentication token *aging* information, such as when the authentication token *expires*, ... number of valid days, and the like; access hours restrictions for the user's account; account expiration date; and account service restrictions, such as what directories, file, resource, or services the user is authorized to access. ..." utilizes expiration as an alarm condition, typically as a result of connection/acknowledgement setup. The examiner broadly interprets the "determining whether the next remote execution process has been running for a first amount of

time, and terminating the next remote execution process when the next remote execution process has been running for at least the first amount of time ... setting a next alarm event when the next remote execution process has been running the second amount of time" as the re-attempting of the authentication process, such that the scenario is effectively a serial authentication process with a alarm condition result reporting aspect.). The involved servers inherently will store data associated with the state(s) of any ongoing processing (i.e., building a formatted message (results of authentication, or re-transmission sequence as applied to the non-acknowledged packet transfer/connection setup state alarm condition result, etc.) prior to communicating such information back through the communications path);

Further, as per claim 25; this claim is the software computer-readable medium claim for the method claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection;

Further, as per claim 37; this claim is the server part of the system claim for the method claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection.

***Conclusion***

17. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

7/25/05